CRIMINAL JUSTICE CONNECTIONS

January/February 2015
Volume 22 Issue 3

An employee publication of the
Texas Department of Criminal Justice

Information Security: Back to the Basics

Every New Year, people resolve to improve themselves by exercising more, eating a healthier diet and becoming more physically fit. TDCJ's Information Security Department would like to add one more resolution to your list: get back to the basics of information security.

Information security can only be implemented using a variety of sophisticated technologies, but regardless of which encryption or anti-virus programs are used, no matter how many firewalls are put into place or how much money is spent for additional layers of technical protection, vulnerabilities due to human failure can never be removed.

To succeed with this resolution, go back to three basics principles of information security:

Physical security

In many ways, physical security is the most critical layer of information security. When others are allowed to follow you or "tailgate" into your building without having to log in or without anyone knowing why they are there, physical security has been breached. Equipment or data could be stolen or destroyed without any knowledge of who committed the act. Securing sensitive information in locked cabinets and behind locked doors will help discourage potential information thieves.

Data encryption

Many of you know that the Information Security Department is in the process of adding encryption software to remove the risk of confidential data being accessed using stolen or misplaced laptop computers. In these cases, if someone tries to access the data without using the correct passphrase, the encrypted laptop locks and turns into a nearly useless paperweight. Encryption also applies to files and email: if confidential data is to be emailed, it should be encrypted. Only a few extra seconds are needed to encrypt a file before sending it, but those few seconds are the difference between secure communication and creating a potentially damaging security breach.

Strong passwords

If your password is weak, the best encryption program in the world won't protect you. Passwords need to be as strong as possible. Using upper and lower-case letters, numerals and punctuation symbols is a good start, but remember that while the most complicated password may seem unbreakable, it isn't if you attach a written copy of it to your monitor or hide it under the keyboard. Change your password frequently, don't leave written copies of it where they can be easily found and don't use the same password for every account.

Resolve to follow these basic security strategies, and you'll help prevent sensitive information from falling into the hands of those who might use it to harm you or the agency. If you have any questions or comments about information security, call the Information Security Department at 936-437-1800.